AMENDMENTS TO THE SPECIFICATION:

Please add the following new paragraph immediately after the title appearing on page 1:

This disclosure is based upon French Application No. 03/03522, filed March 24, 2003, and International Application No. PCT/FR2004/000718, filed March 24, 2004, the contents of which are incorporated herein by reference.

Page 1, immediately prior to line 3, add the following heading:

Background of the Invention

Page 3, immediately prior to line 3, add the following heading:

Summary of the Invention

Page 3, replace the paragraph beginning on line 3 with the following amended paragraph:

The object of the present invention is therefore to increase the protection of this memory against unwanted access, while not slowing down the operation of the circuit.

Page 3, replace the paragraph beginning on line 3 with the following amended paragraph:

According to the invention, a circuit comprises a microprocessor and a set of peripheral devices including at least one communication interface for external access, in which these peripheral devices, unlike the communication interface, are connected to the microprocessor by an interconnection bus on which the data length is equal to the standard data length of the data processed by said microprocessor.

According to the invention, the integrated circuit also comprises a security module connected to the interconnection bus and to the communication interface by a dedicated link, and the length of the data processed by the security module is greater than the standard data length of the data processed by the microprocessor. Therefore, the integrated circuit comprises means for adapting the length of the data processed by the security module to the standard data length. Preferably, the means for adapting the length of the data processed by the security module to the standard data length includes a cache memory, associated with the microprocessor and provided with a cache memory controller which, upon accessing the cache memory, causes it to transmit to the security module data having a length equal to the standard data length. The cache memory is a rapid and efficient means for preparing data to be ciphered by the security module, and also for breaking down ciphered data from the format compatible with the security module, into a format presenting a standard data length, compatible with the data bus of the microprocessor. This allows the processing of the data by the security module to be performed on the fly.

Add the following new paragraphs immediately following the preceding amended paragraph:

During the ciphering of the data by the security module, the cache memory prepares data having a length greater than the standard data length, whereby said data can be accepted at the input of the security module.

On the other hand, during the deciphering of the data by the security module, the cache memory breaks the deciphered data available at the output of the security module and having a length greater than the standard data length, into standard-length data.

This arrangement yields also the advantage of flexibility, since the circuit can process data of a greater or different length than the standard data length, which is particularly advantageous when the data processed by the security module are rather long, which depends on the ciphering algorithm used.

According to a preferred embodiment, the security module uses a secret key algorithm which processes data having a length of at least 64 bits, and the standard length of the data processed by the microprocessor is less than 64 bits.

The secret key algorithm is preferably the AES algorithm.

Delete the paragraphs that begin on page 3, line 15 and ending on page 4, line 2.

Page 4, immediately prior to line 6, add the following heading:

Brief Description of the Drawings

Page 4, immediately prior to line 12, add the following heading:

Detailed Description

Page 5, delete the paragraph beginning on line 14 and ending on line 16.

Page 6, replace the paragraph beginning on line 6 with the following amended paragraph:

Algorithms with a private or secret key will be given preference since they require much less processing time than algorithms with public keys.

Page 8, replace the paragraph beginning on line 6 with the following amended paragraph:

The ~~private~~ secret key used by the algorithm is preferably stored in a so-called OTP register (One Time Programmable). If the integrated circuit IC is provided with a non-volatile flash memory, this register can be located there.